AMENDMENTS TO THE CLAIMS

Please replace the claims, including all prior versions, with the listing of claims below.

Listing of Claims:

1. (Currently Amended) A method for encryption of information for a radio transmission and ~~for~~ authentication of subscribers in a communication system that comprises an access network having equipment for said radio transmission, said communication system ~~further~~ comprising a core network having a respective authentication equipment for said subscriber authentication, comprising ~~the steps of~~:

allocating a radio channel for said transmission of said information via a radio interface from/to a base station of said access network;

mutually transmitting public keys between a mobile station and said base station via said radio interface;

encrypting subsequent information to be transmitted via said radio interface using one of said public keys received by said base station or said mobile station;

deciphering encrypted information received by said mobile station or said base station on the basis of a private key that is allocated to said transmitted, public key in said mobile station or in said base station; and

authenticating said core network via a subscriber identity mobile card of said mobile station, and authenticating said subscribers via said authentication equipment of said core network on the basis of encrypted information that have been mutually sent.

2. (Previously presented) A method according to claim 1, further comprising the steps of:

sending a first public key from said mobile station to said base station;

encrypting information to be sent to said mobile station using said first public key by said base station,

sending an other public key from said base station to said mobile station;

encrypting information to be sent to said base station using said other public key by said mobile station, and

sending a second public key to said base station by said mobile station subsequent to said step of sending said other public key from said base station.

3. (Currently Amended) A method according to claim 2, further comprising ~~the step of~~ replacing said first public key with said second public key sent to said base station.

4. (Currently Amended) A method according to claim 1, further comprising ~~the steps of~~:

sending a first public key from said base station to said mobile system;

encrypting information to be sent to said base station using said first public key by said mobile station;

sending an other public key from said mobile station to said base station;

encrypting information to be sent to said mobile station using said other public key by said mobile station; and

sending a second public key to said mobile station by said base station subsequent to said step of sending said other public key from said mobile station.

5. (Currently Amended) A method according to claim 4, further comprising ~~the step of~~ replacing said first public key with said second public key sent to said base station.

6. (Currently Amended) A method according to claim 1, further comprising ~~the steps of~~ sending a subscriber identity of said subscriber and an authentication request by said mobile station to said core network in encrypted form;

returning, by said authenticating equipment of the core network, an authentication reply in encrypted form; and

implementing, by said mobile station, an authentication procedure for checking an identity of said core network.

7. (Currently Amended) A method according to claim 6, further comprising ~~the steps of~~:

sending an authentication request in addition to said authentication reply [~~(aures-co)~~] in encrypted form by said authenticating equipment of said core network;

returning, by said mobile station, an authentication reply to said authenticating equipment of said core network in encrypted form; and

checking said subscriber identity by an authentication procedure implemented by said authenticating equipment of said core network.

8. (Currently Amended) A method according to claim 1, further comprising ~~the step of~~ implementing said authentication procedure utilizing secret keys.

9. (Currently Amended) A method according to claim 1, further comprising ~~the steps of~~: servicing, by said access network at least two core networks in parallel; and

registering and authenticating in different core networks a subscriber that can use said mobile station in parallel.

10. (Currently Amended) A method according to claim l, further comprising ~~the step of~~:

servicing, by access network, a core network in which a plurality of subscribers that can use said mobile station in parallel are registered and authenticated.

11. (Previously presented) A method according to claim 1, wherein said access network and said core network or multiple core networks are administered by different network operators.

12. (Currently Amended) A communication system for encryption of information for a radio transmission and for authentication of subscribers, comprising:

an access network having equipment for said radio transmission ~~as well as~~and a core network, said core network having a respective authentication equipment for said subscriber authentication, said communication system utilizing a radio channel for transmission of said information via a radio interface from/to a base station of the access network;

memory devices in a mobile station and in said base station for storing public keys and private keys that are allocated to said public keys[,];

transmitters in said mobile station and in said base station for mutually sending said public keys via said radio interface; and

controllers in said mobile station and in said base station for encryption of said information to be subsequently sent via said radio interface upon employment of said public keys received by said base station or, respectively, said mobile station and for deciphering received, encrypted information on the basis of said stored, appertaining private key,

said mobile station comprising a subscriber identity mobile card for authenticating said core network[;], and

said core network comprising an authentication equipment for authenticating said subscribers; and said authenticating said core network and said authenticating said subscribers utilizing mutually transmitted, encrypted information.

13. (Previously presented) A communication system according to claim 12, wherein said access network has at least two core networks connected in parallel for registration and authentication of a subscriber that can use said mobile station in parallel in different core network.

14. (Previously presented) A communication system according to claim 12, wherein said access network has a core network connected for registration and authentication of a plurality of subscribers that can use said mobile station in parallel.

15. (Currently Amended) A communication system according to claim 12, wherein said access network and said core network or multiple core networks are administered by different network operators.